به نام خدا

مباحثی در مقدمات جبر ۱

مولف :

دکتر سودابه تاج نیا

عضو هیئت علمی دانشگاه آزاد اسلامی واحد دزفول

انتشارات ارسطو
(چاپ و نشر ایران)
۱۴۰۱

سرشناسه : تاج‌نیا، سودابه، ۱۳۶۲-
عنوان و نام پدیدآور : مباحثی در مقدمات جبر ۱/مولف سودابه تاج‌نیا.
مشخصات نشر : ارسطو (سامانه اطلاع رسانی چاپ و نشر ایران) ، ۱۴۰۱.
مشخصات ظاهری : ۸۶ ص.
شابک : ۸-۰۳۸-۳۳۹-۶۲۲-۹۷۸
وضعیت فهرست نویسی : فیپا
یادداشت : کتابنامه.
موضوع : جبر -- راهنمای آموزشی (عالی)
Algebra -- Study and teaching (Higher)
جبر -- مسائل، تمرین‌ها و غیره (عالی)
Algebra -- Problems, exercises, etc. (Higher)
رده بندی کنگره : QA۱۵۹
رده بندی دیویی : ۵۱۲/۰۰۷۶
شماره کتابشناسی ملی : ۹۰۹۲۳۲۳
اطلاعات رکورد کتابشناسی : فیپا

نام کتاب : مباحثی در مقدمات جبر ۱
مولف : دکتر سودابه تاج نیا
ناشر : ارسطو (سامانه اطلاع رسانی چاپ و نشر ایران)
تیراژ : ۱۰۰۰ جلد
نوبت چاپ : اول - ۱۴۰۱
چاپ : مدیران
قیمت : ۶۵۰۰۰ تومان
فروش نسخه الکترونیکی - کتاب‌رسان :
https://chaponashr.ir/ketabresan
شابک : ۸-۰۳۸-۳۳۹-۶۲۲-۹۷۸
تلفن مرکز پخش : ۰۹۱۲۰۲۳۹۲۵۵
www. chaponashr. ir

انتشارات ارسطو

مقدمه

کتابی که پیش روی شماست شامل مفاهیم اولیه و مقدماتی جبر مجرد می‌باشد و تلاش شده است که محتوای مطالب جمع‌آوری شده تقریبا تمام سرفصل‌های درس جبر ۱ در رشته ریاضیات و کاربردها را پوشش دهد. همچنین کتاب شامل نکات کلیدی و مهم جهت آمادگی دانشجویان در آزمون کارشناسی ارشد می‌باشد. تمرین‌های ارایه شده برای درک بهتر مفاهیم ضروری است و از صورت برخی تمارین برای اثبات قضیه‌ها استفاده می‌شود. همچنین این کتاب دانشجویان را برای اختیار درس‌های سطح بالاتر ریاضی و کامپیوتر آماده می‌کند.

تنها پیش‌نیاز کتاب داشتن درک کافی از ریاضیات پایه برای دانشجویان می‌باشد.

فهرست مطالب

فصل ۱

نظریه‌ی گروهها

۱.۱ مقدمات و تعاریف اولیه

در این فصل به تعریف و مفاهیم اولیه گروه می‌پردازیم که در واقع یک دستگاه متشکل از مجموعه‌ای ناتهی و یک عمل دوتایی تعریف شده روی آن است. ابتدا برخی از مفاهیم استفاده شده در فصل را تعریف و بیان می‌کنیم.

تعریف **۱.۱.۱**. تابع φ_اویلر یک تابع با دامنه تعریف $\mathbb{N}$ است که چنین تعریف می‌شود: $\varphi(1) = 1$ و به ازای هر $n > 1$، $\varphi(n)$ مساوی تعداد اعداد طبیعی است که از n کوچکتر و نسبت به n اول باشد؛ به‌عنوان مثال: $\varphi(8) = 4$ ، $\varphi(4) = 2$ و اگر p عددی اول باشد: $\varphi(p) = p - 1$.

قضیه **۲.۱.۱**. ۱. به ازای هر دو عدد طبیعی m و n، $(m,n) = 1$ اگر و فقط اگر $\varphi(mn) = \varphi(m)\varphi(n)$.

۲. به ازای هر عدد اول p و هر عدد طبیعی k، $\varphi(p^k) = p^k(1 - \frac{1}{p})$.

نتیجه **۳.۱.۱**. اگر عدد طبیعی n دارای تجزیه یکتای $n = p_1^{l_1}p_2^{l_2}...p_r^{l_r}$ باشد که در آن $p_1 < p_2 < ... < p_r$ اعداد اول و $l_1, l_2, ...l_r$ اعداد طبیعی هستند، آنگاه

$$\varphi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2})...(1 - \frac{1}{p_r})$$

یکی از مفاهیم اساسی در مطالعه‌ی جبر مجرد، مفهوم گروه می‌باشد. در این فصل بطور مختصر به مطالعه‌ی گروهها می‌پردازیم.

تعریف **۴.۱.۱**. دستگاه جبری $(G, *)$ را یک گروه نامند اگر خواص زیر برقرار باشد.

۱. عمل دوتایی $*$ روی G شرکت‌پذیر است، یعنی به ازای هر $a, b, c \in G$، $a*(b*c) = (a*b)*c$.

۲. G دارای عنصر e است یعنی به ازای هر $a \in G$، $a*e = e*a = a$.

۳. هر عنصر G نسبت به $*$، معکوس‌پذیر است یعنی به ازای هر $a \in G$، $b \in G$ای وجود دارد بطوریکه $a*b = b*a = e$

تعریف **۵.۱.۱**. گروه $(G, *)$ را آبلی **(یا جابجایی)** نامند اگر به ازای هر $a, b \in G$، $a*b = b*a$ و در غیر اینصورت گروه را ناآبلی نامند. بدیهی است برای اثبات اینکه گروهی مانند $(G, *)$ ناآبلی است، کافیست نشان دهیم که عناصری مانند $a, b \in G$ وجود دارند بطوریکه

$$a*b \neq b*a$$

تعریف **۶.۱.۱**. فرض کنید $(G, *)$ یک گروه باشد. عدد اصلی مجموعه‌ی G را مرتب G نامند که آن را با $|G|$ نشان می‌دهند. اگر $|G|$ متناهی باشد، G را گروه متناهی و در غیراینصورت آن را گروه نامتناهی نامند.

تبصره **۷.۱.۱**. ۱. اگرچه منظور از یک گروه مجموعه‌ای مانند G همراه با عملی دوتایی همانند $(\times)$ می‌باشد با اینحال معمولاً گروه را فقط با مجموعه‌اش یعنی G نمایش می‌دهند.

۲. برای عملهای دوتایی که با جمع و ضرب متفاوت هستند لزوماً نمادهایی همانند $(*)$ و یا $(\circ)$ را بکار نمی‌برند، بلکه معمول است عملها را برحسب مورد یا همان جمع وضرب نمایش دهند. بنابراین بجای $a*b$ از $a+b$ یا ab استفاده خواهد شد. نوعی توافق نیز وجود دارد که نماد $(+)$ را فقط برای عملهای تعویض‌پذیر بکار رود.

قضیه زیر نشان می‌دهد که عنصر همانی و معکوس هر عنصر در گروه منحصربفرد است. از این‌رو می‌توان نمادهایی مشخص برای نمایش عنصر همانی و معکوس هر عنصر گروه G بکار برد. معمول است در عمل جمع عنصر همانی را با $(\circ)$ و در عمل

ضرب عنصر همانی را با (۱) نمایش دهیم. همچنین در عمل جمع معکوس عنصر $a \in G$ را با $-a$ نشان داده و قرینه a می‌خوانند و در عمل ضرب معکوس عنصر a را با نماد a^{-1} نشان می‌دهند.

قضیه **۸.۱.۱**. فرض کنید G یک گروه باشد. در اینصورت

۱. عنصر همانی G یکتاست.

۲. هر عنصر G دارای معکوس یکتاست.

۳. به ازای هر $a \in G$، $(a^{-1})^{-1} = a$.

۴. به ازای هر $a, b \in G$، $(ab)^{-1} = b^{-1}a^{-1}$.

۵. به ازای هر $a, x, y \in G$،

$$ax = ay \Longrightarrow x = y \qquad \text{(قانون حذف از چپ)}$$
$$xa = ya \Longrightarrow x = y \qquad \text{(قانون حذف از راست)}$$

اثبات. ۱) فرض کنید e و e' عناصر همانی در G باشند. چون e عنصر همانی است، در نتیجه $ee' = e$ همچنین چون e' نیز عنصر همانی است، لذا $ee' = e'$. اما عمل دوتایی یک تابع می‌باشد، از اینرو بایستی $e = e'$.
۲) فرض کنید b و c دو عنصر معکوس برای $a \in G$ باشند. در اینصورت

$$b = ba = b(ac) = (ba)c = ec = c \Longrightarrow b = c$$

۳) بنابر تعریف گروه، $aa^{-1} = a^{-1}a = e$. لذا با استفاده از قسمت (۲)، $a = (a^{-1})^{-1}$.
۴) داریم

$$(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aea^{-1} = e$$

و به همین نحو،

$$(b^{-1}a^{-1})(ab) = e$$

لذا بنابر قسمت (۲) نتیجه می‌شود که $(ab)^{-1} = b^{-1}a^{-1}$.
۵) اگر $ax = ay$، آنگاه

$$a^{-1}(ax) = a^{-1}(ay) \Longrightarrow (a^{-1}a)x = (a^{-1}a)y \Longrightarrow x = y$$

به همین نحو، $xa = ya \Longrightarrow x = y$ $\square$

چند مثال از گروهها

(۱) مجموعه اعداد صحیح $\mathbb{Z}$، نسبت به عمل جمع معمولی یک گروه آبلی است.

(۲) مجموعه‌ی $\mathbb{Q} - \{۰\}$، تحت عمل ضرب معمولی یک گروه آبلی است.

(۳) به ازای هر $n \in \mathbb{N}$، مجموعه همه‌ی رده‌های هم‌ارزی به پیمانه‌ی n، یعنی

$$\mathbb{Z}_n = \{[۰], [۱], ...[n - ۱]\}$$

نسبت به عمل جمع همنهشتی تشکیل یک گروه آبلی از مرتبه n می‌دهد. در این گروه معمولاً $[i]$ را با خود i و یا با $\bar{i}$ نمایش می‌دهیم. با این قرارداد: $\mathbb{Z}_n = \{۰, ۱, ..., n - ۱\}$. بسادگی بررسی می‌شود که $\mathbb{Z}_n$ نسبت به عمل ضرب همنهشتی در حالت کلی تشکیل گروه نمی‌دهد. یا این حال می‌توان ملاحظه کرد که

$$H_n = \{i \in \mathbb{Z}_n \mid (i, n) = ۱\}$$

تشکیل یک گروه ضربی آبلی می‌دهد و $\mid H_n \mid= \varphi(n)$. (یادآوری می‌شود که اگر $(i, n) = (j, n) = ۱$، آنگاه $(ij, n) = ۱$).

(۴) فرض کنید

$$GL_n(\mathbb{R}) = \{(a_{ij})_{n\times n} \mid a_{ij} \in \mathbb{R}, ۱ \leq i, j \leq n\}$$

مجموعه تمام ماتریس‌های معکوس‌پذیر $n \times n$ باشد که درایه‌های آنها از اعداد حقیقی $\mathbb{R}$ هستند. به آسانی می‌توان تحقیق کرد که این مجموعه از ماتریس‌ها نسبت به عمل ضرب ماتریس‌ها تشکیل یک گروه غیرآبلی می‌دهد. $GL_n(\mathbb{R})$ گروه خطی $(generalLinear)$ نامیده می‌شود.
مجموعه ماتریس‌های معکوس‌پذیر $n \times n$ با دترمینان یک را بصورت زیر نشان می‌دهیم؛

$$SL_n(\mathbb{R}) = \{A \in GL_n(\mathbb{R}) \mid det(A) = ۱\}$$

ملاحظه می‌شود که $SL_n(\mathbb{R})$ نیز تحت عمل ضرب ماتریس‌ها تشکیل گروه می‌دهد. این گروه را گروه خطی خاص نامند.

(۵) فرض کنید A مجموعه‌ای ناتهی و $S(A)$ مجموعه همه‌ی توابع دوسویی از A به روی A باشد. عمل دوتایی $(\circ)$ روی $S(A)$ را ترکیب توابع در نظر بگیرید که این عمل بسته دوتایی و شرکت‌پذیر است. تابع همانی $i_A : A \longrightarrow A$ عنصر همانی $S(A)$ است ولذا $S(A)$ ناتهی می‌باشد. به‌علاوه به ازای هر تابع دوسویی $f : A \longrightarrow A$ تابع معکوسی مانند $f^{-1} : A \longrightarrow A$ وجود دارد به‌قسمی که $fof^{-1} = f^{-1}of = i_A$. بنابراین $S(A)$ نسبت به عمل $(\circ)$ تشکیل گروه می‌دهد. $S(A)$، گروه جایگشت A یا $(PermutationGroup)$ نامیده می‌شود و توابع دوسویی روی A را جایگشت‌های A نامند. بخصوص اگر A مجموعه‌ای متناهی با n عنصر باشد، آنگاه گروه جایگشت A را گروه متقارن $(SymmetricGroup)$ روی A نیز نامند و بوسیله‌ی S_n نشان داده می‌شود. به آسانی می‌توان تحقیق کرد که S_n گروهی است متناهی و از مرتبه $n!$. همچنین گروه متقارن S_n ناآبلی است بجز به ازای ۲ یا $n = 1$.

(تمرین۱) فرض کنید $G = \{(a,b) \mid a,b \in \mathbb{R}, a \neq 0\}$ به ازای هر $(a.b),(c,d) \in G$ قانون $(\times)$ را روی G بصورت

$$(a,b) * (c,d) = (ac, bc + d)$$

تعریف می‌کنیم. ثابت کنید $(G,*)$ گروهی ناآبلی است.

(تمرین۲) ثابت کنید که گروه G، آبلی است اگر و فقط اگر به ازای هر $a,b \in G$، $(ab)^2 = a^2b^2$.

(تمرین۳) فرض کنید G یک گروه، و a,b عناصری از G باشند بطوریکه $ab = ba$. به ازای هر $n \in \mathbb{Z}$، ثابت کنید $(ab)^n = a^nb^n$.

(تمرین۴) اگر در گروه G، به ازای سه عدد صحیح متوالی k داشته باشیم $(\forall a,b \in G)(ab)^k = a^kb^k$ ثابت کنید که G گروهی آبلی است.

تعریف **۹.۱.۱**. دستگاه جبری $(S,*)$ را یک نیم‌گروه نامیده می‌شود اگر عمل دوتایی $*$ روی S شرکت‌پذیر باشد، همچنین یک نیم‌گروه با عنصر همانی را یک مونوئید نامند. به عنوان مثال، $(\mathbb{Z},.)$ تشکیل یک مونوئید می‌دهد.

تعریف **۱۰.۱.۱**. اگر $(S,*)$ یک نیم‌گروه و $(n > ۱)$ $a_۱, a_۲, ..., a_n$ عناصری از S باشند، ترکیب این عناصر را به طریق بازگشتی و بصورت زیر تعریف می‌کنیم:

$$a_۱ * a_۲ * ... * a_n = (a_۱ * a_۲ * ... * a_{n-۱}) * a_n$$

به کمک تعریف قبل، قضیه زیر نشان می‌دهد که ترکیب n عنصر در یک نیم‌گروه تنها به ترتیب قرار گرفتن عناصر پشت‌سر هم بستگی دارد و به چگونگی پرانتزگذاری بستگی ندارد.

قضیه **۱۱.۱.۱**. **(تعمیم قانون شرکت‌پذیری)** فرض کنید S یک نیم‌گروه و $(n \geq ۳)$ $a_۱, a_۲, ..., a_n$؛ n عنصر دلخواه از S باشند. در اینصورت کلیه‌ی ترکیب‌های ممکن از $a_۱, a_۲, ..., a_n$ که در آن‌ها ترتیب عناصر یکسان و پرانتزها بصورت دلخواه باشند یکی است.

قضیه **۱۲.۱.۱**. فرض کنید G یک نیم‌گروهی دلخواه باشد. در اینصورت شرایط زیر معادلند:

(الف) G یک گروه است.

(ب) عنصر $e \in G$ وجود دارد بطوریکه به ازای هر $g \in G$، $ge = g$ $(eg = g)$ و بعلاوه به ازای هر $g \in G$ عنصری مانند $g' \in G$ وجود دارد بطوریکه $gg' = e$ $(g'g = e)$.

اثبات. **(الف)** $\longrightarrow$ **(ب)** بدیهی است.

(ب) $\longrightarrow$ **(الف)** کافیست نشان دهیم عنصر همانی راست، عنصر همانی چپ و معکوس راست هر عنصر، معکوس چپ نیز می‌باشد. برای این منظور، فرض کنید $g \in G$ عنصری دلخواه باشد بنابه فرض $g' \in G$ای وجود دارد بطوریکه

$$gg' = e \qquad (۱)$$

همچنین به ازای این $g' \in G$، $g'' \in G$ای وجود دارد به قسمی که

$$g'g'' = e \qquad (۲)$$

اکنون داریم:

$$g'g = g'ge = g'g(g'g'') = g'(gg')g'' = g'eg'' = g'g'' = e$$

یعنی معکوس راست معکوس چپ نیز هست. بعلاوه:

$$eg = (gg')g = g(g'g) = ge = g$$

یعنی عنصر همانی راست، عنصر همانی چپ است. بنابراین G گروه می‌باشد. $\square$

(تمرین) فرض کنید G یک نیم‌گروه باشد. ثابت کنید که گزاره‌های زیر معادلند:

الف) G یک گروه است.

ب) به ازای هر $a,b \in G$، معادلات $ax = b$ و $ya = b$ دارای جواب یکتا هستند.

(حل): (الف $\longleftarrow$ ب) بدیهی است که $x = a^{-1}b$ یک جواب معادله‌ی $ax = b$ می‌باشد. حال فرض کنید $x' \in G$ جواب دیگری از این معادله باشد، یعنی $ax' = b$. در اینصورت داریم $ax' = a(a^{-1}b)$ که در نتیجه $x' = a^{-1}b$، یعنی جواب یکتاست.
در مورد معادله $ya = b$ نیز به همین نحو عمل می‌شود.

(ب $\longleftarrow$ الف) فرض کنید $a.$ عنصر ثابتی از G باشد. در معادله $ax = b$ قرار می‌دهیم $a = b = a.$، در اینصورت عنصری مانند $e \in G$ جوابی از معادله $a.x = a.$ می‌باشد. اکنون فرض کنید a عنصر دلخواهی از G باشد. معادله $ya. = a$ دارای جواب $y.$ است یعنی $y.a. = a$. در نتیجه

$$ae = (y.a.)e = y.(a.e) = y.a. = a$$

بنابراین e عنصر همانی راست است. حال به ازای هر $b \in G$، معادله‌ی $bx = e$ دارای جواب است یعنی $b' \in G$ای وجود دارد به قسمی که $bb' = e$ پس هر عنصر G دارای معکوس راست است. از اینرو بنابر قضیه‌ی بالا، G یک گروه است.

تعریف **۱۳.۱.۱**. فرض کنید G گروهی ضربی باشد و $x \in G$. دراینصورت به ازای هر $n \in \mathbb{N}$ تعریف می‌کنیم:

$$x^{\cdot} = e$$
$$x \text{ام}n \text{توان} = x^n = (x^{n-1})x \quad , \quad x^{-n} = (x^{-1})^n$$

قضیه **۱۴.۱.۱**. اگر G گروهی ضربی یا جمعی باشد، آن‌گاه به ازای هر $m,n \in \mathbb{Z}$ و هر $x \in G$؛

۱. $(x^m)^n = x^{mn} \quad , \quad x^m x^n = x^{m+n}$ **(حالت ضربی)**

۲. $n(mx) = (nm)x \quad , \quad mx + nx = (m+n)x$ **(حالت جمعی)**

فرض کنید G گروهی دلخواه باشد. بعضی از زیرمجموعه‌های ناتهی G خواص خود گروه را حفظ می‌کنند، یعنی با قانون ترکیب گروه تشکیل یک گروه می‌دهند. این زیرمجموعه‌ها را زیرگروه نامند. به عبارت دقیق‌تر

تعریف **۱.۱.۱۵**. فرض کنید G گروهی ضربی و H زیرمجموعه‌ای ناتهی از G باشد. اگر H نسبت به عمل دوتایی تعریف شده در G تشکیل یک گروه دهد، آن‌گاه H را زیرگروهی از G نامند که با نماد $H \leq G$ نشان می‌دهیم. اگر e عنصر همانی گروه G باشد، آن‌گاه $\{e\}$ و خود G، زیرگروه‌هایی از G هستند که آن‌ها را زیرگروه‌های بدیهی G نامند. هر زیرگروه متمایز از G را زیرگروه سره نامند.

(تمرین) فرض کنید G یک گروه باشد و $H \leq G$. ثابت کنید:

(۱) $e_H = e_G$

(۲) به ازای هر $h \in H$ معکوس h در H همان معکوس h در G است.

(حل): (۱) فرض کنید e_G و e_H بترتیب عناصر همانی G و H باشند. دراینصورت چون e_H عنصر همانی در H است در نتیجه $e_H e'_H = e'_H$. از طرفی چون e_G عنصر همانی G و $e_H \in G$. در نتیجه $e_G.e_H = e_H$. لذا در G داریم:

$$e_H e_H = e_G e_H \quad \Longrightarrow \quad e_H = e_G$$

(۲) به‌عهده‌ی خواننده واگذار می‌شود.

قضیه‌ی زیر یک شرط لازم و کافی برای زیرگروه بودن بدست می‌دهد.

قضیه **۱.۱.۱۶**. فرض کنید G یک گروه باشد و $\phi \neq H \subseteq G$. دراینصورت $H \leq G$ اگر و فقط اگر به ازای هر $a, b \in H$ و $ab^{-1} \in H$.

اثبات. اگر $H \leq G$، واضح است که به ازای هر $a, b \in H$ اولاً $b^{-1} \in H$ و ثانیاً $ab^{-1} \in H$. برعکس: فرض کنید به ازای هر $a, b \in H$ و $ab^{-1} \in H$. بویژه $aa^{-1} = e \in H$ و بنابراین $eb^{-1} = b^{-1} \in H$. یعنی عنصر همانی گروه G متعلق به H است و معکوس هر عنصر H در H است. همچنین H نسبت به عمل G بسته است، زیرا $a(b^{-1})^{-1} = ab \in H$. خاصیت شرکت‌پذیری در H همانند G برقرار است از اینرو H زیرگروه G است. $\square$

(تمرین) فرض کنید G گروهی دلخواه و H زیرمجموعه‌ای ناتهی و متناهی از G باشد. ثابت کنید $H \leq G$ اگر و فقط اگر به ازای هر $a, b \in H$، $ab \in H$.

چند مثال از زیرگروهها

(۱) قبلاً ملاحظه شد که مجموعه‌های $\mathbb{Z}$، $\mathbb{Q}$، $\mathbb{R}$ و $\mathbb{C}$ نسبت به عمل جمع و $\mathbb{Q}^\star$، $\mathbb{R}^\star$ و $\mathbb{C}^\star$ نسبت به عمل ضرب گروه هستند. به آسانی ملاحظه می‌شود که زنجیرههای زیرگروه‌های زیر برقرارند.

$$\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C} \quad , \quad \mathbb{Q}^\star \leq \mathbb{R}^\star \leq \mathbb{C}^\star$$

باید توجه کرد که خاصیت زیرگروه بودن متعدی است. از اینرو مثلاً $\mathbb{Z} \leq \mathbb{C}$.

(۲) به ازای هر $n \geq ۲$، $SL_n(\mathbb{R}) \leq GL_n(\mathbb{R})$.

(۳) به ازای هر $n \in \mathbb{Z}$، مجموعه‌ی $n\mathbb{Z} = \{nm \mid m \in \mathbb{Z}\}$ زیرگروهی از $(\mathbb{Z}, +)$ می‌باشد.

قضیه **۱۷.۱.۱**. اگر $\{H_i\}_{i\in I}$ خانواده‌ای از زیرگروه‌های G باشد، آن‌گاه $\bigcap\limits_{i\in I} H_i$ نیز زیرگروهی از G است.

اثبات. چون به ازای هر $i \in I$ و $e \in H_i$، در نتیجه $e \in \bigcap\limits_{i\in I} H_i$. پس $\bigcap\limits_{i\in I} H_i \neq \phi$. اگر $x, y \in \bigcap\limits_{i\in I} H_i$ عناصری دلخواه باشند، آن‌گاه به ازای هر $i \in I$، $x, y \in H_i$؛ از اینرو بنا به قضیه‌ی بالا به ازای هر $i \in I$، $xy^{-۱} \in H_i$. بنابراین $xy^{-۱} \in \bigcap\limits_{i\in I} H_i$ لذا $H \leq G$. □

ممکن است این سوال به نظر آید که آیا اجتماع دو زیرگروه نیز یک زیرگروه است؟ در مثال زیر نشان می‌دهیم که این مطلب در حالت کلی نادرست می‌باشد.
مثال نقض: در گروهی جمعی $\mathbb{Z}$ می‌دانیم که $۲\mathbb{Z}, ۳\mathbb{Z} \leq \mathbb{Z}$. در صورتیکه $D = ۲\mathbb{Z} \bigcup ۳\mathbb{Z}$ نمی‌تواند زیرگروه $\mathbb{Z}$ باشد، زیرا $۲ \in D$ و $۳ \in D$ ولی $۲ + ۳ \notin D$. یعنی D نسبت به عمل جمع بسته نیست.

(تمرین ۱) اگر K و H زیرگروه‌هایی از G باشند. ثابت کنید که $H \bigcup K \leq G$ اگر و فقط اگر $H \subseteq K$ یا $K \subseteq H$.

(تمرین ۲) نشان دهید که هیچ گروهی را نمی‌توان بصورت اجتماع دو زیرگروه سره‌ی متمایز آن نوشت.

(تمرین ۳) فرض کنید G گروهی دلخواه باشد. ثابت کنید که $\mathbb{Z}(G) = \{x \in G \mid xg = gx, \forall g \in G\}$ زیرگروهی از G است. ($Z(G)$ را مرکز G یا $CenterSubgroup$ می‌نامند.)

(تمرین ۴) فرض کنید G گروهی دلخواه باشد و $g \in G$. ثابت کنید که

$$g^{-1}Hg = \{g^{-1}hg \mid h \in H\} \leq G$$

($g^{-1}Hg$ را زیرگروه زوج H در G می‌نامند.)

(تمرین ۵) فرض کنید G یک گروه باشد و $H \leq G$. ثابت کنید که

$$C_G(H) = \{g \in G \mid gh = hg, \forall h \in H\} \leq G$$

($C_G(H)$ را مرکزساز H در G می‌نامند.)

(تمرین ۶) اگر G گروهی آبلی باشد و $n \in \mathbb{N}$، ثابت کنید که

$$H = \{x \in G \mid x^n = e\} \leq G$$

قضیه **۱۸.۱.۱**. فرض کنید G یک گروه و A زیرمجموعه‌ای از G باشد. در اینصورت زیرگروهی از G وجود دارد که A را شامل بوده و کوچکترین زیرگروه G با این خاصیت است.

اثبات. چون G به‌عنوان یک زیرگروه از خودش شامل A است. در نتیجه فرض کنید K اشتراک تمام زیرگروههایی از G باشد که A را دربردارند یعنی

$$K = \bigcap_{A \subseteq H \leq G} H$$

□

بنابر قضایای گذشته، K زیرگروهی از G است و همچنین واضح است که $A \subseteq K$. اکنون فرض کنید T زیرگروهی از G شامل A باشد. دراینصورت طبق تعریف K، $K \subseteq T$.

تعریف **۱۹.۱.۱**. (زیرگروه تولیدشده توسط یک زیرمجموعه از گروه) فرض کنید G یک گروه و A زیرمجموعه‌ای از G باشد. کوچکترین زیرگروه G که A را دربردارد، زیرگروه تولیدشده بوسیله‌ی A نامیده می‌شود و با نماد $< A >$ نشان داده می‌شود در حالی‌که $A = \{a_۱, a_۲, ..., a_n\}$ مجموعه‌ای متناهی باشد، آن‌گاه مختصراً می‌نویسیم $< A >=< x_۱, x_۲, ..., x_n >$ بویژه اگر $A = \{a\}$، آن‌گاه زیرگروه $< a >$ را زیرگروه دوری G نامند. سرانجام اگر به ازای یک زیرمجموعه‌ی A از G، داشته باشیم $G =< A >$، آن‌گاه A را یک مجموعه‌ی مولد G می‌نامیم؛ و درصورتیکه $G =< x_۱, x_۲, ..., x_n >$، می‌گوییم G گروه متناهیاً تولیدشده است. واضح است که $\{e\} =< \phi >$.

قضیه‌ی زیر کمک موثری برای شناخت عناصر $< A >$ می‌باشد:

قضیه **۲۰.۱.۱**. فرض کنید G یک گروه ضربی و A زیرمجموعه‌ای ناتهی از آن باشد دراینصورت:

$$< A >= \{a_۱^{\alpha_۱} a_۲^{\alpha_۲} ... a_n^{\alpha_n} \mid n \in \mathbb{N}, a_i \in A, \alpha_i \in \{-۱, ۱\}\}$$

نتیجه **۲۱.۱.۱**. فرض کنید G گروهی آبلی و A زیرمجموعه‌ای ناتهی از آن باشد. دراینصورت در حالت ضربی

$$< A >= \{a_۱^{k_۱} a_۲^{k_۲} ... a_n^{k_n} \mid a_i \in A, n \in \mathbb{N}, k_i \in \mathbb{Z}\}$$

و در حالت جمعی

$$< A >= \{k_۱ a_۱ + k_۲ a_۲ + ... + k_n a_n \mid a_i \in A, n \in \mathbb{N}, k_i \in \mathbb{Z}\}$$

نتیجه **۲۲.۱.۱**. فرض کنید G یک گروه و $a \in A$. دراینصورت در حالت ضربی

$$< a >= \{na \mid n \in \mathbb{Z}\} \text{ ، } < a >= \{a^n \mid n \in \mathbb{Z}\}$$

(مثال) در گروه جمعی $\mathbb{Z}$، زیرگروه تولیدشده بوسیله‌ی $\{۲\}$ عبارتست از:

$$< ۲ >= \{۲k \mid k \in \mathbb{Z}\}$$

و زیرگروه تولیدشده توسط $\{۲, ۳\}$ عبارتست از:

$$< ۲, ۳ >= \{۲k + ۳l \mid k, l \in \mathbb{Z}\}$$

همچنین در گروه ضربی $Q^\star = Q - \{۰\}$، زیرگروه تولیدشده به‌وسیله‌ی $\{۳, \frac{۱}{۲}\}$ چنین است:

$$<3, \frac{1}{2}> = \{3^k(\frac{1}{2})^l \mid k, l \in \mathbb{Z}\}$$

(تمرین) در گروه $\mathbb{Z}_{12}$ زیرگروههای تولیدشده توسط مجموعه‌ی $\{2\}$ و $\{3\}$ و $\{6\}$ را مشخص کنید.

(قضیه‌ی لاگرانژ و نتایج آن)

اگر H زیرگروهی از G باشد، چون H و G دارای ساختار جبری یکسانی هستند از اینرو به نظر می‌آید که تقریباً دارای خواص مشترکی باشند. به‌عنوان مثال دیده می‌شود که اگر G آبلی باشد آن‌گاه H نیز آبلی است. حال در این قسمت به ارتباط بین مرتبه‌های G و H هنگامی که G گروهی متناهی است می‌پردازیم. در ابتدا چند تعریف و قضیه را مورد مطالعه قرار می‌دهیم:

عمل دوتایی ضربی تعریف‌شده روی عناصر یک گروه را می‌توان به زیرمجموعه‌های آن نیز تعمیم داد. اگر A و B دو زیرمجموعه‌ی ناتهی از گروه G باشند، آن‌گاه حاصلضرب AB چنین تعریف می‌شود:

$$AB = \{ab \mid a \in A, b \in B\}$$

در حالت‌های خاص مفهوم حاصلضرب از اهمیت ویژه‌ای برخوردار است. بخصوص وقتی A تنها شامل یک عنصر و B زیرگروهی از G باشد.

تعریف **۲۳.۱.۱**. فرض کنید G یک گروه و H زیرگروهی از آن باشد. به ازای عنصر $a \in G$، مجموعه‌ی $ah = \{ah \mid h \in H\}$ را یک همرده‌ی چپ H در G و مجموعه‌ی $ha = \{ha \mid h \in H\}$ را یک همرده‌ی راست H در G نامند، که در هر مورد a را نماینده‌ی همرده در نظر می‌گیریم.

قضیه‌ی زیر مبین آن است که مجموعه همرده‌های راست یک زیرگروه در آن گروه تشکیل یک افراز می‌دهد.

قضیه **۲۴.۱.۱**. فرض کنید G یک گروه و H زیرگروهی از آن باشد. دراینصورت

۱. به ازای هر $g \in G$، $g \in Hg$.

۲. به ازای هر $g_1, g_2 \in G$، $g_1 \in Hg_2$ اگر و فقط اگر $Hg_1 = Hg_2$.

۳. به ازای هر $g_1, g_2 \in G$، یا $Hg_1 = Hg_2$ یا $Hg_1 \bigcap Hg_2 = \phi$.

۴. $G=\bigcup_{g\in G} Hg$

اثبات. (۱) به ازای هر $g\in G$، داریم $g=eg\in Hg$
(۲) فرض کنید $g_۱\in Hg_۲$. دراینصورت به ازای $h\in H$ای، $g_۱=hg_۲$. در نتیجه به ازای هر $h'\in H$

$$h'g_۱=h'(hg_۲)=(h'h)g_۲\in Hg_۲$$

از اینرو $Hg_۱\subseteq Hg_۲$. به‌همین نحو می‌توان نشان داد که $Hg_۲\subseteq Hg_۱$. بنابراین $Hg_۱=Hg_۲$. عکس این مطلب بسادگی از قسمت(۱) نتیجه می‌شود.
(۳) اگر به ازای عناصری مانند $g_۱,g_۲\in G$، $Hg_۱\bigcap Hg_۲\neq\phi$، آن‌گاه $g\in G$ای وجود دارد به‌قسمی که $g\in Hg_۱$ و $g\in Hg_۲$. حال بنابر (۲)، $Hg_۱=Hg=Hg_۲$.
(۴) بدیهی است. $\square$

تبصره **۲۵.۱.۱**. همانند قضیه‌ی بالا می‌توان نشان داد که مجموعه‌ی همرده‌های چپ نیز تشکیل یک افراز برای گروه می‌دهند.

(مثال ۱) همرده‌های راست $<۲>$ در گروه جمعی $\mathbb{Z}$ عبارتند از

$$<۲>=<۲>+۰=۲\mathbb{Z}\quad,\quad <۲>+۱=\{۲k+۱\mid k\in\mathbb{Z}\}$$

(مثال ۲) با توجه به مثال‌های قبل، اگر S_n گروه متقارن روی مجموعه‌ی $\{۱,۲,۳,...,n\}$ باشد. نمادگذاری زیر در انجام محاسبات کمک موثری می‌کند. جایگشتی که ۱ را به $r_۱$ و ۲ را به $r_۲$ و بطورکلی i را به r_i تبدیل کند بصورت زیر نشان می‌دهیم؛

$$\begin{pmatrix} ۱ & ۲ & ۳ & ... & n \\ \downarrow & \downarrow & \downarrow & ... & \downarrow \\ r_۱ & r_۲ & r_۳ & ... & r_n \end{pmatrix}$$

و یا جایگشتی که $r_۱$ را به $r_۲,...,r_{m-۱}$ را به r_m و r_n را به $r_۱$ تبدیل کند $(m\leq n)$ و بقیه‌ی اعداد را ثابت نگه دارد بصورت زیر نشان می‌دهیم:

$$\begin{pmatrix} r_۱ & r_۲ & r_۳ & ... & r_n \end{pmatrix}=\begin{pmatrix} r_۱ & r_۲ & ... & r_n \\ r_۲ & r_۳ & ... & r_۱ \end{pmatrix}$$

اکنون عناصر $S_۳$ را بدست می‌آوریم و سپس جدول ضرب آن را می‌نویسیم:

$$S_۳ = \left\{ e = \begin{pmatrix} ۱ & ۲ & ۳ \\ \downarrow & \downarrow & \downarrow \\ ۱ & ۲ & ۳ \end{pmatrix} = (۱), a = \begin{pmatrix} ۱ & ۲ & ۳ \\ \downarrow & & \\ ۱ & ۳ & ۲ \end{pmatrix} = (۲ \quad ۳), b = \begin{pmatrix} ۱ & ۲ & ۳ \\ ۳ & ۲ & ۱ \end{pmatrix} = (۱ \quad ۳), \right.$$

$$\left. c = \begin{pmatrix} ۱ & ۲ & ۳ \\ ۲ & ۱ & ۳ \end{pmatrix} = (۱ \quad ۲), p = \begin{pmatrix} ۱ & ۲ & ۳ \\ ۲ & ۳ & ۱ \end{pmatrix} = (۱ \quad ۲ \quad ۳), q = \begin{pmatrix} ۱ & ۲ & ۳ \\ ۳ & ۱ & ۲ \end{pmatrix} = (۱ \quad ۳ \quad ۲) \right\}$$

با توجه به اینکه ضرب در S_n همان ترکیب توابع است. ما عمل ترکیب توابع fog را نخست با اثر f و سپس g بدست می‌آوریم. بعنوان مثال:

$$pb = (۱ \quad ۲ \quad ۳)(۱ \quad ۳) = c$$
$$a^۲ = (۲ \quad ۳)(۲ \quad ۳) = e$$

ملاحظه می‌شود که $a^۲ = b^۲ = c^۲ = e$ و $p^۳ = q^۳ = e$. همچنین

$$(۱ \quad ۲ \quad ۳) = (۳ \quad ۱ \quad ۲) = (۲ \quad ۳ \quad ۱)$$

در اینجا جدول ضرب کامل گروه متقارن $S_۳$ را درج می‌کنیم:

	e	a	b	c	p	q
e	e	a	b	c	p	q
a	a	e	q	p	a	b
b	b	p	e	q	a	c
c	c	q	p	e	b	a
p	p	b	c	a	q	e
q	q	c	a	b	e	p

حاصلضرب xy بدین ترتیب محاسبه شده است که x از سمت چپ سطر و y از بالای ستون جدول در هم ضرب شده‌اند. ملاحظه می‌شود که هر عنصر $S_۳$ در هر سطر یا ستون جدول فقط یکبار ظاهر شده است. این مطلب در هر گروهی برقرار است و نتیجه‌ای است از این امر که در هر گروه به ازای عناصر مفروض d و t، معادله‌ی $dx = t$ یا $(xd = t)$ دارای جواب یکتاست.

حال زیرگروه $< a >= \{e, a\}$ را از $S_۳$ در نظر بگیرید. کلیه‌ی همرده‌های راست H در $S_۳$ عبارتند از:

$$H = He = \{e, a\} \quad Hb = \{b, q\} \quad Hc = \{c, p\} \quad bH = \{b, p\}$$

اگرچه در مثال بالا ملاحظه شد که همرده‌ی راست Hg لزومی ندارد با همرده‌ی چپ gH مساوی باشد، با این حال در قضیه‌ی زیر نشان می‌دهیم که اندازه‌ی آن‌ها یکسان می‌باشد.

قضیه **۲۶.۱.۱**. فرض کنید H زیرگروهی از یک گروه G باشد و $g_1, g_2 \in G$، دراینصورت بین هر جفت از مجموعه‌های $eH = H$، g_1H، g_2H و Hg_2 تناظری ۱ − ۱ برقرار است.

اثبات. بسادگی بررسی می‌شود که توابع

$$\begin{array}{ll} \varphi : g_1H \longrightarrow g_2H & \psi : g_1H \longrightarrow Hg_2 \\ g_1h \longmapsto g_2h & g_1h \longmapsto hg_2 \end{array}$$

دوسویی می‌باشند. $\square$

نتیجه **۲۷.۱.۱**. فرض کنید G گروهی متناهی باشد و $g \in G$ دراینصورت به ازای هر $g \in G$،

$$| gH |=| Hg |=| H |$$

قضیه **۲۸.۱.۱**. اگر H زیرگروهی از گروه G باشد، آن‌گاه بین مجموعه همرده‌های راست H در G و مجموعه همرده‌های چپ H در G تناظری دوسویی وجود دارد.

اثبات. فرض کنید $\mathfrak{R}$ و $\mathfrak{L}$ بترتیب مجموعه تمام همرده‌های راست و چپ H در G باشد. رابطه‌ی φ بصورت زیر تعریف می‌کنیم:

$$\varphi : \mathfrak{R} \longrightarrow \mathfrak{L}$$

اولاً φ خوش‌تعریف و ۱ − ۱ است؛ زیرا

$$\forall x \in G \quad Hx \longmapsto x^{-1}H$$

$$\forall x, y \in G \quad Hx = Hy \Longleftrightarrow x \in Hy \Longleftrightarrow xy^{-1} \in H \Longleftrightarrow \exists h \in H \quad s.t \quad xy^{-1} = h \Longleftrightarrow x = hy \Longleftrightarrow x^{-1} = y^{-1}h^{-1} \Longleftrightarrow x^{-1} \in y^{-1}h^{-1} \Longleftrightarrow x^{-1}H = y^{-1}H \Longleftrightarrow \varphi(Hx) = \varphi(Hy)$$

ثانیاً به‌وضوح φ پوشاست. بنابراین φ تناظری دوسویی است. $\square$

از قضیه‌ی بالا تعریف زیر بدست می‌آید.